AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An X.509 certificate stored on a computer readable storage medium for interpretation on a computer apparatus supporting reading of the certificate and control of network cryptographic operation according to the certificate, said certificate capable of supporting more than one cryptographic algorithm with an associated public key, comprising:

a signature algorithm and signature for all authenticated attributes including a first public key associated with a first cryptographic algorithm;

a first certificate extension identifying at least one alternative cryptographic algorithm and providing a respective associated public key; and

a second certificate extension containing a signature for each alternative cryptographic algorithm, whereby an alternative cryptographic algorithm may be supported without establishing a new certificate hierarchy.

2. (Previously Presented) An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

3. (Previously Presented) An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

4. (Previously Presented) A method for enabling an X.509 certificate to support more than one cryptographic algorithm, with an associated public key, comprising the steps of:

providing the X.509 certificate with a signature algorithm with associated public key and signature for all authenticated attributes;

providing the X.509 certificate with a first certificate extension identifying at least one alternative cryptographic algorithm and providing a respective associated public key; and

providing the X.509 certificate with a second certificate extension which contains a signature for each alternative cryptographic algorithm, whereby an alternative cryptographic algorithm may be supported without establishing a new certificate hierarchy.

5. (Previously Presented) The method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

6. (Previously Presented) The method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

7. (Previously Presented) Computer readable code stored on computer readable media for enabling an X.509 certificate to support more than one cryptographic algorithm in association with a public key, said computer readable code comprising:

first subprocesses for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes including a first public key using a first cryptographic algorithm;

second subprocesses for providing the X.509 certificate with a first certificate extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

third subprocesses for providing the X.509 certificate with a second certificate extension which contains a signature for each alternative cryptographic algorithm.

8. (Previously Presented) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

9. (Previously Presented) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

10. (Previously Presented) In a computing environment, a system for enabling an X.509 certificate to support more than one cryptographic algorithm, said computer readable code comprising:

means for providing the X.509 certificate with a signature for all authenticated attributes including a first public key using a first cryptographic algorithm;

means for providing the X.509 certificate with a first certificate extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

means for providing the X.509 certificate with a second certificate extension which contains a signature for each alternative cryptographic algorithm.

11. (Previously Presented) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and second certificate extensions are identified as non-critical.

12. (Previously Presented) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

13. (New) An X.509 certificate according to Claim 1, wherein

the signature for all authenticated attributes includes the signing of the second certificate extension, and

the signature for each alternative cryptographic algorithm does not include the signing of the second certificate extension.

14. (New) The method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein

the signature for all authenticated attributes includes the signing of the second certificate extension, and

the signature for each alternative cryptographic algorithm does not include the signing of the second certificate extension.

15. (New) Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein

the signature for all authenticated attributes includes the signing of the second certificate extension, and

the signature for each alternative cryptographic algorithm does not include the signing of the second certificate extension.

16. (New) A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein

the signature for all authenticated attributes includes the signing of the second certificate extension, and

the signature for each alternative cryptographic algorithm does not include the signing of the second certificate extension.